



# G Data

## マルウェアレポート

2009年下半期

G Dataセキュリティラボ

ラルフ・ベンツミュラー & サブリナ・バーケンコフ

(瀧本往人・岸本眞輔 訳)



Go safe. Go safer. G Data.

# 概要

## 2009年下半期の動向

**半年で90万件** 2009年下半期に発見された新種マルウェアの数は、924,053件でした。これは、2009年上半期よりも39%多く、2008年下半期よりも60%多い数字です。

**年間160万件** 2009年1年間に発見された新種マルウェアの数は、1,588,005件でした。これは、2008年よりも78%多い数字であり、史上最高の数となりました。

**主流はトロイの木馬** 大量のマルウェアが発生するなか、トロイの木馬が、マルウェア全体の42.6%を占めました。2009年上半期と比べると、9.0%上昇しました。トロイの木馬以外で2009年上半期における構成比よりも上昇したのは、ワーム、エクスプロイトおよびウイルスでした。

**PDFウイルスの増加** PDFを使用するマルウェア数は、ほぼ3倍となりました。

**アドウェアの減少** 新しいアドウェアは、25%低減しました。

**減少するマルウェア「種」** マルウェアの数が増える一方で、マルウェア種の数は減少傾向にあります。マルウェア種（ファミリー）は年間で、2,908件が登場しました。2008年は3,069件でした。最も数の多かったマルウェア種は、順に、ゲノム（Genome、2009年上半期3位）、ピーシークライアント（PcClient、新登場）、フピゴン（Hupigon、2009年上半期1位）です。

**主流は変わらずウィンドウズ** ウィンドウズは、今なおマルウェア攻撃の主要な標的となっており、99.0%を占めました。ドットネット（.NET）のマルウェアは、2009年上半期と比べると、0.3%に減少しました。ウェブアプリケーションのためのスクリプト言語のマルウェアは、0.5%で、ほぼ横ばいでした。

## 2010年の予測

**裏経済需要のマルウェア** 裏経済において特定の役割のあるダウンローダー、バックドア、およびルートキットについては、2009年とほぼ同様の割合で発生するでしょう。

**エクスプロイト** 数多く登場するおそれがあります。

**ウェブアプリケーション** 攻撃のための、より重要な目標になりつつあります。

**SNSに注意** マイスペース（MySpace）やフェイスブック（Facebook）、ツイッター（Twitter）などのソーシャルネットワークは、スパムのプラットフォームとして、また、犯罪活動を準備したり実行するための情報源として引き続き使用されるでしょう。

**データ窃取** 利益のあがるビジネスであることが止むことはないでしょう。そのため、銀行を狙うトロイの木馬、スパイウェア、およびキーロガーの発生率が下がる見込みはありません。



## 2010年のトピック

**クープフェイス**   クープフェイス (Koobface) は発生後1年がすぎて、これまで以上の攻撃が見られます。

**ガンブラー**    現在、最大のウェブページを感染させるマルウェアとして注目されます。

**データ保護**    情報漏えいならびにデータプロテクションの違反が数多く発生し、クレジットカードと金融部門を含む信用ビジネスへの信頼性が低下しつつあります。

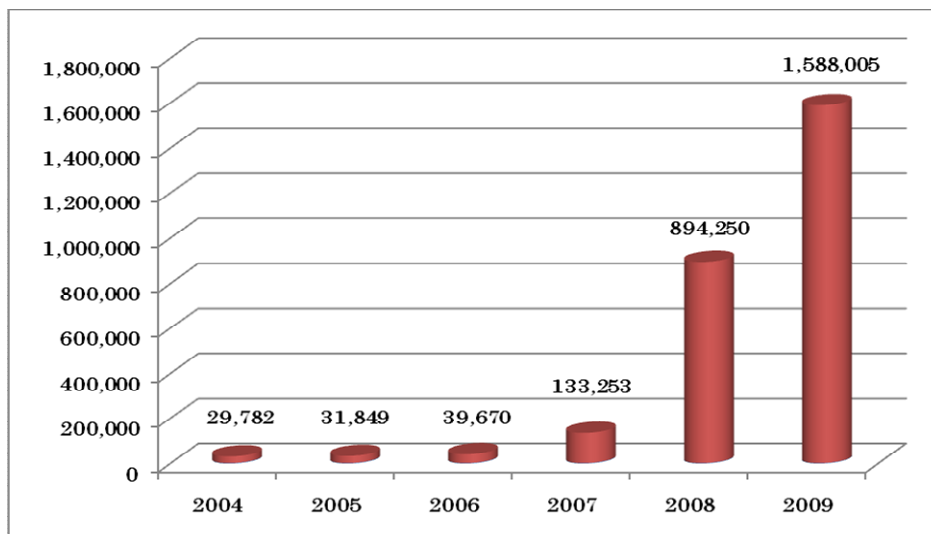
# 目次

概要	2
2009 年下半期の動向	2
2010 年の予測	2
2010 年のトピック	3
マルウェア基本情報	5
無限成長？	5
マルウェアカテゴリー別状況	6
マルウェア種別状況	7
プラットフォーム別マルウェア発生状況	9
2010 年の見通し	11
2010 年上半期の動向予測	11
ウェブ 2.0: ソーシャルネットワーク	12
データ保護問題	15
2009 年下半期の出来事とトレンド	16
2009 年 7 月	16
2009 年 8 月	16
2009 年 9 月	17
2009 年 10 月	18
2009 年 11 月	19
2009 年 12 月	20

# マルウェア基本情報

## 無限成長？

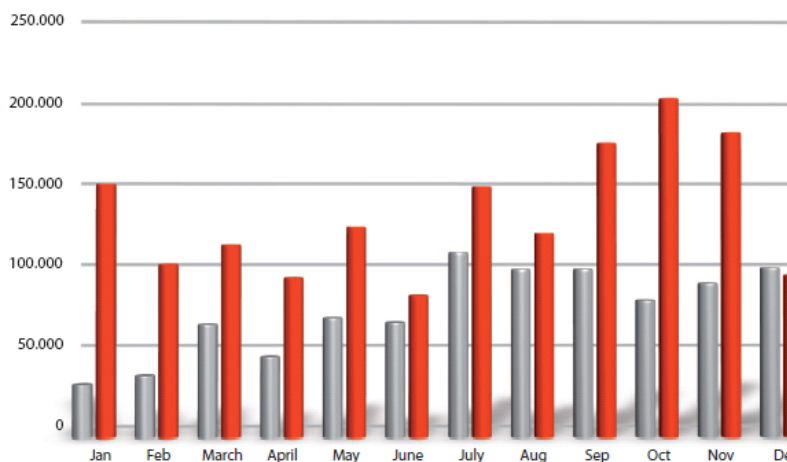
新種マルウェアの数は、表1に示されているように、ここ数年驚くべき勢いで増加し続けています。2009年下半期もまた、924,053件という記録的な数字となりました。\*この総数の計算は、悪性コードを含むファイルを一つずつ数え上げたものではありません。あくまでもワクチン側から見たものです。



グラフ1 新種マルウェア数の変遷（2004～2009）

2009年上半期と比べても、39%の増加率となりました。ただし、2008年の下半期からの増加率が60%であったのと比べると、上昇率については下がりました。

2009年1年間の合計数にすると、1,588,005件でした。2008年と比べると、78%の増加率です。2004年において1年間に発見された新種マルウェア数が、2009年では、わずか1週間分で発生したことになります。



グラフ2 月別マルウェア数の変遷（赤 = 2009年、グレー = 2008年）

## カテゴリー別状況

カテゴリー別にみると、トロイの木馬が、近年において最もよく登場するマルウェアとなっています。2009年下半期においても、大きくその数が上昇しました。表1で示されているように、全体に占める割合は42.6%であり、上半期よりも9.0%高い割合でした。

マルウェア全体の数としては、2009年の上半期よりも39%上昇しました。2008年の下半期から60%上昇したのと比べると、動きはやや緩やかになっています。

しかしながら、ダウンローダー（27%上昇）、バックドア（32%上昇）、およびツール（27%上昇）が増加したことには、注意が必要です。なぜならば、これらのマルウェアのカテゴリーは、裏市場で主要なウイルスとして扱われているものだからです。

ダウンローダーは、ウイルスを大量にばらまくのに使用されており、バックドアは、コンピュータの遠隔操作（ボットネット）を可能にします。ツールは、初心者がこのマルウェアの世界に参入しやすくしており、また、専門家が日々の業務を行うための手助けにもなっています。

また、最も増加率が高かったのは、ワームです。上半期と比べると約2倍（96%上昇）、2008年下半期と比べるとほぼ3倍（197%上昇）になりました。これは、大部分がバスン（Basun）の増加によるものです。バスンは一時期減少していましたが、以前は上位10位に入っていたものです。上半期では、ワームの中でもオートラン（Autorun）が頻出しました。

エクспロイトの数も、全体の平均上昇率よりも高く増加しました。上半期と比べると50%、昨年の同期と比べると85%増でした。これは、CVE（共通脆弱性識別子）として登録されたセキュリティホールの数かなり減少しているのと比べると対照的です。脆弱性報告は、2008年には7,250であったのに対して、2009年は4,594と約半分程度に減少しています。報告された脆弱性の数が減っている一方で、マルウェアに悪用される数は増加しているのです。

とりわけ広く利用されているソフトウェアについては、そのセキュリティホールが狙われる傾向にあり、インターネットを通してコンピュータを攻撃する際に頻りに利用されるようになってきました。バージョンアップをしていないソフトウェアを使っているコンピュータは、サイバー犯罪者たちにとって、格好の餌食なのです。

	2009年下半期		2009年上半期		上半期との差	2008年下半期		前年下半期との差
	数	比率	数	比率	比率	数	比率	比率
トロイの木馬	393,421	42.6%	221,610	33.6%	+78	155,167	26.9%	+154
ダウンローダー/ドロッパー	187,958	20.3%	147,942	22.1%	+27	115,358	20.0%	+63
バックドア	137,958	14.9%	104,224	15.7%	+32	125,086	21.7%	+10
スパイウェア	86,410	9.4%	97,011	14.6%	-11	96,081	16.7%	-10
ワーム	51,965	5.6%	26,542	4.0%	+96	17,504	3.0%	+197
アドウェア	30,572	3.3%	34,813	5.3%	-12	40,680	7.1%	-25
ツール	14,516	1.6%	11,413	1.6%	+27	7,727	1.3%	+88
ルートキット	11,720	1.3%	12,229	1.9%	-4	6,959	1.2%	+68
エクспロイト	3,412	0.4%	2,279	0.3%	+50	1,841	0.3%	+85
(狭義の)ウイルス	637	0.1%	143	0.0%	+345	167	0.0%	+281
ダイアラー	415	0.0%	1,153	0.2%	-64	1,013	0.2%	-59
その他	5,543	0.5%	4,593	0.7%	+21	8,419	1.5%	-34
計	924,053	100.0%	663,952	100.0%	+39	576,002	100.0%	+60

表1 マルウェア発生数と割合（2009年下半期、上半期、2008年下半期）

しかしながら上半期よりも著しく増加したのは、狭義のウイルスでした(345%上昇)。近年はあまり使われることもなく縮小傾向にあったのですが、このカテゴリーには実行ファイルを攻撃する古典的なファイル感染型ウイルスが含まれており、USBメモリスティックや他のポータブル外部記憶デバイスの普及が上昇をもたらしました。とはいえマルウェア発生数全体に占める割合は0.1%にすぎず、大流行には至りませんでした。

他方、スパイウェアは新種が減少傾向にあります。9.4%を占めるにすぎませんでした。2009年の上半期が14.6%であったのに対して、5.2%下がりました。昨年の下半期が16.7%であったのに対して、7.3%も下がりました。といっても、もうデータが盗まれなくなったということではありません。むしろ正反対です。スパイ機能は、単体機能しか持たないスパイウェアとして分類されるのではなく、トロイの木馬として、包括的なパッケージに統合されているのが現状だからです。

ルートキットは、スパイウェアとバックドアの機能を巧みに隠蔽するものです。2009年の上半期には、かなり増加し、今や要注意のマルウェアですが、新種にかぎって言えば、若干減少傾向にあります。

それに対してアドウェアは、かなりの減少となりました。この、広告を行う目的のマルウェアは、前年の下半期との比較では25%も減少しました。2009年上半期に最も多く発生したウイルス種であるモンダー(Monder)の新種発生数が激減したのが、主な理由と考えられます。2009年下半期には、モンダーはトップ10以下にまで下がりました。

## マルウェア種別状況

2009年の下半期には、2,200種のマルウェアが活動しました。マルウェアは、その機能と特性によって、種別に分類できます。この数年間、マルウェアプログラムの数は大変な勢いで増加してきましたが、種別数は着実に下がってきた、というのが特徴です。つまり、亜種の発生数が圧倒的に多くなりました。

2008年の上半期には、マルウェア種は、2,395ありました。それが下半期には、2,094となりました。さらに2009年の上半期には1,948にまで下がりました。ところが2009年下半期には、マルウェアの種別数は、再び増加しました。

ただし年度でみると、2008年には3,069のマルウェア種が発生しましたが、2009年は2,908でした。したがって、大枠では種別数は減り、特定のマルウェア種が集中的に使用される傾向が続いている、と言えます。

	2009 年下半 期	マルウェア種	2009 年上半 期	マルウェア種	2008 年下半 期	マルウェア種
1	67,249	ゲノム	34,89	モンダー	45,407	フピゴン
2	38,854	ピーシークライアント	26,879	フピゴン	35,361	オンラインゲーム
3	37,026	フピゴン	18,576	ゲノム	20,708	モンダー
4	35,115	スカー	16,719	ブザス	18,718	モンダーB
5	24,164	ブザス	16,675	オンラインゲームズ	15,937	シンマス
6	20,581	リプラ	13,889	フラウドロード	13,133	ブザス
7	19,848	マガニア	13,104	ピフローズ	13,104	マガニア
8	18,645	レフレッソ	11,106	ポイズン	12,805	ピーシークライアント
9	16,271	サフィス	10,322	マガニア	11,530	ズイーロブ
10	16,225	バスン	10,312	インジェクト	10,412	パーチュモンド

表2 最も活動的なマルウェア種ベスト10 (2009年下半期、上半期、2008年下半期)

表2では、この1年半で最も多くの亜種を発生させたマルウェア種が示されています。2009年の下半期では、ゲノムが最も多く、1日に184の亜種が登場しました。また、2番目のピーシークライアント(PcClient)や3番目のフピゴン(Hupigon)などのバックドアは、1日に平均100以上の亜種が生まれます。

## 上位マルウェア種の概要

新種発生の多かったマルウェア種について、以下で簡単に説明します。

### ゲノム (Genome)

トロイの木馬型で、ダウンローダー、キーロガー、ファイル暗号化の機能が統合されたものです。

### ピーシークライアント (PcClient)

バックドア型で、コンピュータを遠隔操作してデータを盗み出すのに使用されます。ファイルと登録エントリーを隠すためにルートキット技術を使用しています。

### フピゴン (Hupigon)

バックドア型で、攻撃者はコンピュータを遠隔操作します。キーボード入力の記録や、ファイルシステムへのアクセス、ウェブカメラへのアクセスを可能にします。

### スカー (Scar)

トロイの木馬型で、ダウンローダー、スパイウェア、ボットなど、マルウェアの更なるダウンロードを開始するのに使用されるテキストファイルをロードします。

### ブザス (Buzus)

トロイの木馬型で、個人情報(クレジットカード、オンラインバンキング、EメールおよびFTPアカウント)を探し出し攻撃者にデータを転送します。そのうえ、より容易に犠牲者のコンピュータを攻撃できるようにコンピュータのセキュリティ設定を下げようと試みます。

### リブラ (Lipler)

ウェブサイトから追加マルウェアをダウンロードできるダウンローダーを含みます。またブラウザのスタートページを変えます。

### マガニア (Magania)

トロイの木馬型で、台湾のガマニア社のオンラインゲームのパスワードを盗むために用いられ、何度も圧縮したRAR形式のメールの添付ファイルに紛れて侵入を試みます。画像を表示し注意を逸らしているあいだにバックグラウンドで別のファイルをシステムにロードします。また同時に、インターネット・エクスプローラーにDLLを登録し、攻撃者がいつでもネット利用をモニタリングできるようにします。

### リフレソ (Refroso)

新たに上位に入ってきたトロイの木馬型ウイルスです。2009年6月の終わり頃に最初に発見されました。バックドアの機能を用い、ネットワークで他のコンピュータを攻撃します。

### サスフィス (Sasfis)

このトロイの木馬は、コンピュータ上にファイルをインストールし、インターネットから新たなマルウェアをダウンロードするのを試みます。亜種はメール添付として送られてきます。

### バスン (Basun)

2年ぶりに、ワームが10位以内に入りました。現在のユーザーが管理者の名でPCに侵入します。ローカルネットワークで他のコンピュータを攻撃し、感染を広げます。

## プラットフォーム別発生状況

### あくまでもウィンドウズが主流

近年のマルウェア作成者の攻撃は、ウィンドウズ・プラットフォームに集中していました。大半のマルウェアはウィンドウズのために開発されてきたために、新種マルウェアのなかでウィンドウズが占める割合は、たえず増加してきました。ところが2009年の下半期は、ウィンドウズは99.0%を占め、わずかに割合が下がりました（表3を参照）。

ただし、このわずかに減少した理由は、マルウェアが3番目に多かったプラットフォームとかかわりがあります。MSIL（共通中間言語）でつくられたマルウェアが、大きく増加したのです。上半期と比べて、数にすると、365から2,732に、比率にすると、0.1%から0.3%に上昇しました。

MSILは、ドットネット（.NET）言語で書かれたプログラムをコンパイル変換したもので、プラットフォームやプログラミング言語に依存しないフォーマットです。マルウェア作成者もまた、まさしくこのドットネット環境を悪用する機会が増えています。ドットネットアプリケーションの大部分は、ウィンドウズでホストされているのです。

2番目に多かったのは、ジャバ・スクリプト（JavaScript）、PHP、ASP HTMLなどを含むウェブページのスクリプト（WebScript）で、連続して0.5%の割合を維持しました。ウェブページによる感染は、最近人気を集めている、と言えるでしょう。

このウェブスクリプトをプラットフォームとしたマルウェア、総数4,371のうちの3,295は、ジャバ・スクリプトのマルウェアでした。と言ってもジャバ・スクリプトは、ウェブページにインストールされるわけではありません。1,624のマルウェアプログラムは、拡散媒体としてPDFを使用しています。

PDFに基づくマルウェアプログラム、通称「PDFウイルス」は、2008年には780ありました。2009年にはその数は2,394まで増加しました。ほとんど3倍になったのです。

	プラットフォーム	2009年下半期		2009年上半期		2008年下半期	
		発生数	構成比	発生数	構成比	発生数	構成比
1	Win32	915,197	99.0%	659,009	99.3%	571,568	99.2%
2	WebScript	4,371	0.5%	3,301	0.5%	2,961	0.5%
3	MSIL	2,732	0.3%	365	0.1%	318	0.1%
4	Script	1,124	0.1%	924	0.1%	1,062	0.2%
5	NSIS	229	0.0%	48	0.0%	58	0.0%
6	Mobile	120	0.0%	106	0.0%	70	0.0%

プラットフォーム別マルウェア発生数トップ5（2009年下半期、上半期、2008年下半期）

\* 「WebScript」は、ジャバ・スクリプト、HTML、フラッシュ/ショックウェーブ、PHPまたはASPに基づいているマルウェアを指します。通常はブラウザ経由で脆弱性を突くマルウェアを意味します。「Script」は、VBS、パール（Perl）、パイソン（Python）またはルビー（Ruby）といったスクリプト言語に書かれているバッチ、シェルスクリプトまたはプログラムです。「MSIL」は、ドットネット・プログラムのバイトコードで保存されたマルウェアです。「NSIS」は、ウィンプ（Winamp）によって使用されるインストールプラットフォームです。「Mobile」は、J2ME、シンビアン（Symbian）、およびウィンドウズCEのためにマルウェアを含みます。

ウィンドウズのマルウェアと比べるとそれほど数が多いはありませんが、これまで目立たなかったNSISプラットフォームのマルウェアが著しく増加し、トップ5に入りました。2009年上半期が48だったのに対して下半期は229も発見されました。

それに対して、モバイルをプラットフォームとしたマルウェア数は、120だったため、順位を下げました。なお、モバイルは本来別々に分けて言及することもできますが、それほど数が多くないので一つにとりまとめています。

NSISは、ウインアンブ・メディアプレーヤーなどをインストールするのに使用されるインストールプラットフォームです。インストールプラットフォームとしてのNSISの人気はフリーウェアだからであり、商用のソフトウェア開発者に基づいたものではありません。

## ユニックスとマックのウイルス発生状況

表3にはありませんが、ユニックス (nix) ベースのシステムについては、37のマルウェアプログラムが現れました。2009年の上半期が66だったのと比べると、減少しました。

アップルのマックOSの新しいマルウェアプログラムは、わずか3つ発見されたにとどまりました。

ニュースなどではマックのウイルスが登場すると大きく話題としてとりあげられますが、ウィンドウズの大量のマルウェア数と比べると、その割合は、きわめて少ないと言えます。

# 2010年の見通し

近年、マルウェアは、金銭を目的として使用されるのが主です。この傾向はしばらく変わることはないでしょう。裏経済では巨額が動いているために、マルウェアの拡散や攻撃、偽装などについての新たな技術開発も進んでいます。この傾向は、ソーシャルネットワーキングや、モバイル機器、ゲーム機器、そしてマイクロソフト以外のOSなどのウイルス開発も可能としています。ウィンドウズ以外をターゲットとした攻撃も、何度か試される実験によって実際に有効であると判明されれば、サイバー犯罪者は確実にその分野に集中攻撃を行って来ることでしょう。現時点でその兆候がほとんどないとはいえ、たえず注意は必要です。







したがって、当面マルウェアの大量発生は、止むことはありません。この裏市場の定番商品であるダウンロードやバックドア、ツール、およびルートキットは、より洗練された方法で活用されることでしょう。

ネット犯罪者たちの手口として、一般的なデスクトップアプリケーションにおけるセキュリティホールは、今後もお利用され続けることでしょう。発見されるセキュリティホールの数が減少し、ソフトウェア開発者がセキュリティ知識を増やしたとしても、ウェブアプリケーションにおける集中攻撃は避けようもありません。

ソフトウェアに人気があり、インターネットでの使用が増えれば増えるほど、サイバー犯罪者にとっては、そうやって使用されたウェブアプリケーションをハイジャックするのが、より有利になります。同じことは、クラウドコンピューティングのような形で使用されるコンピュータのためのオプションの場合にもあてはまります。ウェブアプリケーションの開発者が、現在デスクトップ・ソフトウェアのために確立されているセキュリティの基本を、クラウド型に対してどこまで適用させようとしているのかについては、まだ明らかになっていないのです。

2010年には、新しいオペレーティングシステムとコンピュータプラットフォームが発売されるという予告は、すでにアナウンスされています。私たちは、これらに対して、裏市場がどうそれらに応じるかを様子見しなければなりません。可能性としては、アップル、ユニックスおよびポータブル・コンピュータのマルウェアプログラム数が増加するかもしれません。特に、ウィンドウズ7の64ビット版がそれほど浸透しないようであれば、マルウェア作成者の動向も変化する可能性があります。

## 2009年下半年期の動向予測

カテゴリー	動向
トロイの木馬	
バックドア	
ダウンロード/ドロッパー	
スパイウェア	
アドウェア	
狭義のウイルス/ワーム	
ツール	

カテゴリー	動向
ルートキット	
エクスプロイト	
Win32	
Web Script	
Script	
MSIL	
Mobile	

# ウェブ2.0: ソーシャルネットワーク

登場した当初、一部の専門家のための専門的な道具だったインターネットは、近年では、毎日普通に用いる道具になるという変貌をとげました。今では、世界中で4人に1人がインターネットを用いるまでに至っています。この数字そのものが、興味深いものです。\* [www.internetworldstats.com](http://www.internetworldstats.com)に従えば、世界中で1,733,933,741人のインターネットユーザーがいることになります。これは、世界中の人口の約25%に相当します。

しかしまた、世界最大規模のソーシャルネットワークコミュニティであるフェイスブック (Facebook) のユーザー数を見ているならば、現在オンラインコミュニティがどれだけのインターネット使用の割合を占めているのかが明らかになるでしょう。

フェイスブックの創設者であるマーク・ザッカーバーグの声明によれば、2009年12月の時点におけるフェイスブックへの登録者数は、3億5000万人を突破していました。これは、統計上で言えば、5人のインターネットユーザーのうちの1人が、アメリカのウェブ2.0プロバイダーに個人情報を提供している、ということになります。\* 出典: <http://blog.facebook.com/blog.php?post=190423927130>

さらに言えば、ウェブ2.0アプリケーションは、ソーシャルネットワークにはとどまらず、さらに広がりがあります。グーグルのドックス (Google Docs) や地図、ピカサ (Picasa)、フリッカー (Flickr)、アイデンティ・カ (Identi.ca)、ジャイク (Jaiku) などは、ウェブ共有のほんの一例にすぎません。多様にあるウェブ2.0アプリケーションはいずれも、非常に関心が高く持たれており、かつ、実際に有用性が高いのも事実です。しかしセキュリティの面から言えば、各サービスはそれ自身の危険性を表に出していません。ユーザーが自分の個人情報をコミュニティページに載せており、しかもその数はあまりにも膨大です。これが危険なのは言うまでもありません。また、問われるのは、これらのプラットフォームの技術的な構造です。私たちが他にも繰り返し見ているように、サイバー犯罪者たちの攻撃は、とどまることを知りません。にもかかわらずネットワークには、それぞれが個別のターゲットとして狙われるようなアプリケーションがますます数多く実装されようとしているのです。

## 一例にすぎないフェイスブック

コミュニティの例としてあげるなら、フェイスブックは顕著に、多くの攻撃にさらされ、ユーザーに不便さをももたらしました。ネットワークのプライバシー設定が相変わらず甘い点と、若年層に多い希薄な保護意識は別としても、至るところでユーザーは危険性と隣合わせにいます。

たとえば2009年11月中旬に、200以上のフェイスブックのグループが「コントロール・ユア・インフォ」(Control Your Info) と名乗る組織に乗っ取られ、名前などの情報が書き換えられる、という事件が起こりました。

どうやら彼らは、セキュリティホールへの注意喚起のために、実際には無害なこの活動を行ったようでした。フェイスブックにハッキングする必要さえなく、グループの内容を変更してしまいました。コントロール・ユア・インフォは、それぞれのグループの管理人を除去しつつ、自分たちの登録を行いました。グループ名と内容を変えるのは、かなり注意を必要とすべきでしょう。しかしながら、攻撃者もまた、たとえば不



法な内容のコンテンツを掲出するならば、何も知らないユーザーが自分の評判を下げてしまうという事態も起こりえます。グループの管理者はグループ内のメンバーすべてにメッセージを配布し、スパムその他を拡散させます。

## 友だちの輪がスパムの輪に

フェイスブックのアドレス帳またはグループからのコンタクトによって送られたメッセージは、大部分のユーザーにとっては、安全なもののみなされています。しかしながら、ハイジャックされたグループや友人を通してスパムが許可なく送られてくることは、はじめから想定しておいたほうがよいでしょう。ただ信じるよりも、しっかりとチェックをすべきです。特に、おもしろビデオやショッキングな写真、または最新情報といった内容であれば、なおのこと注意が必要です。

それらのコンテンツには、リンクが付加されています。このリンクをクリックすると、コンピュータが多種多様な方法で感染するおそれがあります。たとえば、よく知られているのは、おもしろ動画を見るために新たなコーデックが必要だからとそそのかしてウイルスをダウンロードさせる手法です。また、巧妙なやり方としては、ただリンク先を開いただけで感染してしまうドライブバイ・ダウンロード型のウイルスを仕掛けるという手口もあります。また、長年詐欺メールに使用されていた古典的な罠が、今あらためてソーシャルネットワークで使用されはじめています。フェイスブックのユーザーには、一見信頼関係があるように思わせるようなトリックがしばしば用いられています。



## 大量発生したクーブフェイス

ワームの一種であるクーブフェイス (Koobface) は、2008年の年末に発生し、その後、1年以上にわたって盛んに活動してきました。2009年のあいだ中、アンチウイルスのプロバイダーは戦々恐々としていました。クリスマス時期には、「SantA」と呼ばれるビデオの配布がありました。ビデオをクリックすると、ウェブページから必要なコーデックをダウンロードするよう、誘導されます。この偽のコーデックをインストールすると、クーブフェイスが犠牲者のコンピュータに侵入します。同様のやり方で、ソーシャルネットワーク全体に影響を与える場合もあります。

2009年下半期にクーブフェイスは、フェイスブックにはじまり、次々とさまざまなソーシャルネットワークに攻撃を仕掛けてゆきました。例えば、マイスペース (MySpace) やハイファイブ (Hi5) のユーザーも危険であることには変わりありません。

スカイプでも類似例が発見されました。トロイの木馬型で、感染したウェブページを通じてまき散らされ、スカイプユーザーのログインデータを盗み、スカイプアドレス帳からデータを読むものです。

## ツイッターへの攻撃も注意が必要

マイクロブログ・サービスのツイッター（Twitter）は、仲間と交流しあえるウェブアプリケーションのなかでも、もっとも人気の高いものの一つです。しかしながら、いつでもどこでもツイッターを使いたいという欲求は、むしろ、新しいセキュリティホールをもたらしています。2009年8月に、ツイッターのあるアカウントは、Base64形式でコード化された短いメッセージを使用することで、ボットネットを制御するのに使用されました。ツイッター側は、ただちに、このアカウントを停止しました。

また、この短いメッセージログサービスにおいては、感染の別のリスクが、ショートURLサービスから発生します。ユーザーは、もしかすると感染してしまうかもしれないにもかかわらず、省略された部分は見ることができません。よく知られたURL省略サービスは、TinyURL、bit.ly、is.gd、tr.im、およびtwi.bzなどがあります。このショートURLは、きわめて危険なので、ユーザーは、見えている部分だけで信じるべきではないでしょう。ツイッターのアカウントがハイジャックされているなら、簡単にユーザーを罠に誘いこむことができてしまいます。ショートURLをクリックする前に、ユーザーは、それぞれのサービスで提供されている安全対応策を利用すべきでしょう。

ここに、よく知られているサービスのいくつかのサンプルと情報ページのURLを掲げておきます。

	ショートURL	アクション	URL プレビューオプション
TinyURL	<a href="http://tinyurl.com/yzuwcwd">http://tinyurl.com/yzuwcwd</a>	プレビュー	<a href="http://preview.tinyurl.com/yzuwcwd">http://preview.tinyurl.com/yzuwcwd</a>
bit.ly	<a href="http://bit.ly/7jH8xP/info">http://bit.ly/7jH8xP/info</a>	bit.lyのあとに /info	<a href="http://bit.ly/info/7jH8xP">http://bit.ly/info/7jH8xP</a>
is.gd	<a href="http://is.gd/5yGtz">http://is.gd/5yGtz</a>	URLのあとに -	<a href="http://is.gd/5yGtz-">http://is.gd/5yGtz-</a>
twi.bz	<a href="http://gdata.de.twi.bz/b">http://gdata.de.twi.bz/b</a>	URLのあとに -	<a href="http://gdata.de.twi.bz/b/e">http://gdata.de.twi.bz/b/e</a>
tr.im	<a href="http://tr.im/lqpj">http://tr.im/lqpj</a>		

表4 ショートURLとプレビューオプション

## 結論

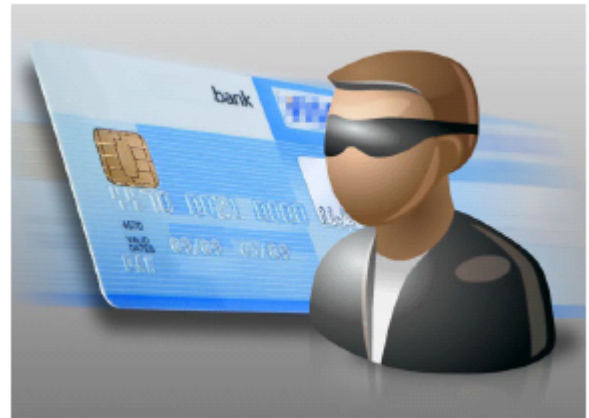
ウェブ2.0のアプリケーションに対する攻撃は、止むことなく、拡大し続けています。闇市場のディーラーや偽装を行う犯罪者たちにとっては、ウェブ2.0に絡む攻撃ツールへの関心は高く、有益な商品であり、これからも価値が高いことは間違いありません。2009年に発生したマルウェアの新しい亜種は、これからも広まり続けることでしょう。そして、マルウェア作成者は、なお一層、ポータルやAPIにおける脆弱性を新たに探し出し、攻撃するための開発にいそむはずで

# データ保護問題

2009年下半期においては、問題の半数以上は、データ保護の部門にかかわっていました。この領域で報告された問題は、範囲が広く、データ窃盗もあれば、不法監視もあります。データ窃盗に関して言えば、データの紛失が、コンピューター・システムのセキュリティホールによってなのか、外部の攻撃者による他の電子装置を用いたものなのか、または内部の仕業でデータの削除が行われたのか、こういった手口を区別する必要があります。

コンピューターのデータの紛失に関して、もっとも大きな問題は、いったんデータが流出してしまうと、無制御に配布されてしまい、そうなってしまうと、もう取り返しがつかないということです。被害者は、データがコピーされるのを止める機会を、ほとんど持つことはできません。

2009年11月に起こった大きな出来事に、スペインのクレジットカードサービスでの個人情報流出がありました。主にドイツとイギリスの顧客の10万件以上のクレジットカードが被害にあいました。書き換えられたカードの数は全体からみればわずかな比率でしたが、この事件によってデジタル情報の危険性が露見したと言えるでしょう。クレジットカード情報は、あらゆる場所で盗むことができるのです。



店頭で支払いを済ませる際、用意されたカードリーダーのデバイスは、カードからデータをコピーする。PCから、例えば、オンラインショッピングを利用しているときに、キーロガーやスパイウェアによってデータを得る。

改ざんされたウェブサイト（フィッシング詐欺を目的とした）上、または、罾を仕掛けた偽装ウェブショップにおいて、フォームにデータを入力するように要求される。

オンラインショップ、支払いサービスおよび銀行のデータベースは保護が不十分であるにもかかわらず取引データを含んでいるため、SQLインジェクションなど、攻撃は何度も繰り返し試みられる。

クレジットカード所有者は、データ処理の場面すべてを統御できるというわけではありません。実際に、被害はあちこちで発生しています。そうなると、危険だからといってクレジットカードを使わなければよい、と考えはじめる人もいますが、それは得策であるとは思えません。これだけネット通販が充実しているなかで、それを使わない手はありません。むしろ、クレジットカード所有者は、リスクを十分に認識しながら、そういった攻撃者から身を守る努力をすべきです。

PCのオペレーティングシステムとブラウザを常に最新に保つ。

性能の高いインターネットセキュリティ製品をインストールし、たえず最新の状態で使用する。

データをフォームに入力するとき、サイトオペレーターが要求する情報が本当に必要なものかどうかをチェック。代金を支払うことがはっきりしているときのみ、暗証番号（PIN）、使い捨てパスワード（TAN）、パスワード、およびクレジットカードのセキュリティコード（CCV）を入力する。

重要なデータは、https、すなわち、暗号化を前提にして送信する。

# 2009年下半期の出来事とトレンド

2009年下半期も SNS への攻撃関連が増加しました。ツイッター、マイスペース、フェイスブックは、フィッシング攻撃者にとって格好の攻撃対象で、マルウェア拡散に悪用されています。

## 2009年7月

7月1日 ツイッター・バグ月間プロジェクトのスタート。2006年からこのプロジェクトに参加するアビブ・ラフ (Aviv Raff) 氏がウェブ 2.0 の脆弱性を公開し、ユーザーやプログラマーに警鐘を鳴らしました。同プロジェクトにおいて氏は、攻撃可能なツイッターのブラウザ API や URL 省略サービス、ワーム型不正コードを仕掛けた画像に焦点を当てました。

7月4日 独立記念日にアメリカと韓国への大規模なサイバー攻撃が行われました。両国政府のセキュリティ専門家が DDoS 攻撃への対応に追われました。何万ものゾンビ PC を従えたボットネットが、両国の公的機関、金融機関、民間企業など (例: ニューヨーク証券取引所、韓国の銀行) のウェブサイトを攻撃しました。北朝鮮がこの攻撃に関わっているものと推測する情報機関もありましたが、真相は定かではありません。

7月8日 エクスプロイト・ポータル Milw0rm が閉鎖を発表しました。理由は明らかではないものの、専門家の間では、エクスプロイト数の増加に伴い、管理者側がキャパシティを超えたとの見方が強くなっています。

7月9日 南アフリカの銀行が ATM のスキミング対策に乗り出し、ATM に催涙スプレー発射装置を設置するも、技術者の保守の際に作動し、技術者 3 人が病院に搬送されました。



7月23日 アドビ社のアクロバット及びフラッシュプレイヤーのコンポーネントである authplay.dll に未知の脆弱性が見つかりました。この脆弱性は、感染した PDF ファイルやドライブバイ・ダウンロード経由での感染を狙う不正ウェブサイトでの悪用が見つかります。

## 2009年8月

クーブフェイス発生から 1 年が経過するも、その攻撃性は衰えません。

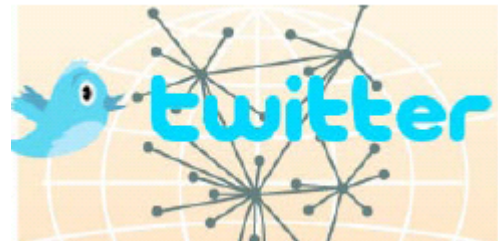
8月4日 BSI (ドイツ連邦情報局) から送付されたメールと見せかけたスパムメール経由で、スケアウェアのサイトに誘導する詐欺被害が発生しました。誘導先のサイトで契約すると、2 年契約で 192 ユーロもの額を請求されました。

8月6日 ツイッターのサービスが数時間にわたりタイムアウトになりました。メインアプリケーション

と API クライアント両方に影響が出ました。原因は、DDoS 攻撃、しかもロシア KGB による「Cyxymu」というプログラマーへの特定の個人に対するスパムメール経由の攻撃と考えられています。

8月13日 マイクロソフトが重大な脆弱性の存在を把握していたにもかかわらず、2年間それを放置していたことが判明しました。2007年7月のパッチデーへの対応を、ずっと先延ばししていました。

8月14日 ツイッターがボットネットのコミュニケーターとしての悪用される可能性があることが話題になりました。アーバーセキュリティ (Arbor Security) の研究者が、あるアカウントの暗号化されたつぶやきにボットネットの指令が含まれていたと発表しました。



8月24日 スtockホルムの地方裁判所は、インターネットのサービスプロバイダーであるブラック・インターネット (Black Internet) に対し、大手ビットトレント (BitTorrent) 検索サイトのパイレーツ・ベイ (The Pirate Bay) への接続停止と、50万スウェーデン・クローナ (約48,000ユーロ) の罰金の支払いを言い渡しました。その後、パイレーツ・ベイは別のISPを見つけました。

8月27日 あるセキュリティ企業でかつて社員として働いていた人物がスカイプを盗聴するための不正コードを発表しました。コードを仕掛けられると、情報が録音され、MP3フォーマットで第三者に送付される仕組みです。

8月29日 中国で、ウィンドウズ XP やその他のソフトウェア不正コピーを行ったとして、不正な複製と配布をした4名に対し、禁固刑および160万USドルの罰金の判決が言い渡されます。

## 2009年9月

9月4日 ドイツ最大手プロバイダーであるT-Onlineのユーザーのメールが数日間利用不能になりました。ボット攻撃で大量メールの送付が原因でした。

9月8日 オーストリアで消防局の管理センターと消防員、救急サービスと搬送の暗号化されていない通信が不正に記録され、出勤先、患者、その他の出勤関連情報の流出が発覚しました。

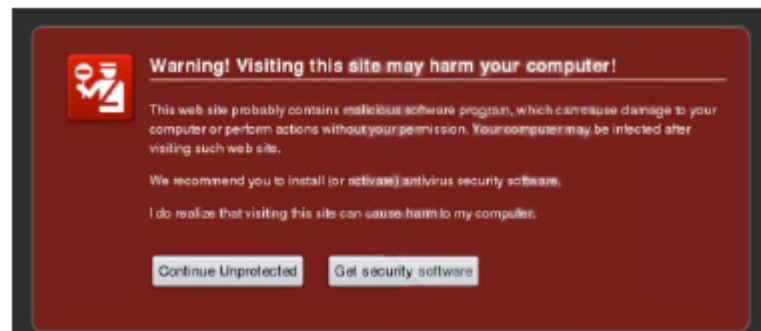
9月14日 ニューヨーク・タイムズ誌のウェブサイト訪問者が、ソーシャルエンジニアリング攻撃の犠牲者になりました。攻撃者はスケアウェアのパナーをホームページ上に表示し、偽ウイルス対策ソフトの購入に導きました。

9月15日 国連特別報告者のナジャ・ムジド・マーラ (Najat M'jid Maalla) が、児童ポルノ関連のウェブサイトが著しい増加を示していると報告しました。サイト数は、2003年から2007年の5年間で4倍増。ユニセフの試算によると、その数は400万にも上ります。

9月16日 アメリカで、PC2台を盗難された男が、リモートアクセスプログラムで取り返しました。RAアクセスで盗難者のネット閲覧、チャット、メールを監視し、それを動画として記録し、警察の捜査に貢献しました。

9月18日 マイクロソフトが、広告を悪用するマルバタイジング (Malvertising) を行う企業を提訴しました。不正コードが含まれる疑わしいパナーに対する初の審理となりました。

9月21日 トロイの木馬 (Trojan.FakeAlert.BFW) に感染すると、偽のセキュリティ警告が表示され、パーソナル・アンチウイルス (Personal Antivirus) というスケアウェアのインストールへと誘導されました。



## 2009年10月

10月1日 フェイスブックのキャプチャ (動画) がクラッカーに破られました。プロフィールを自動で作成される危険性が広がりました。

10月2日 グーグルはパイレート・ベイやビットトレント関連の7サイトを検索結果から削除しました。

10月6日 マイクロソフトのライブホットメール (Live Hotmail) から1万ユーザー分のアカウントとパスワードのリストが流出しました。データはフィッシング攻撃で盗み出された模様です。その後、ヤフー、ジーメール (Gmail)、コムキャスト (Comcast)、アースリンク (Earthlink) も被害にあっていたことが判明しました。

10月7日 FBI 長官であるロバート・ミュラー (Robert Mueller) が危うくフィッシングの被害者にあうところでした。フィッシングメールがさらに巧妙化しました。

10月8日 FBI が国際フィッシング組織を摘発し、詐欺容疑者100人を起訴しました。エジプトのハッカーが個人情報や銀行口座情報を盗みだし、これをアメリカの協力者へ送付、アメリカでは別の犯罪に利用されていました。

10月8日 De-Mail の6ヶ月稼働テストがベルリンでスタートしました。これは、法律遵守かつ信頼できるメールの送受信を実現したものです。

10月9日 バハマ・ボットネット (Bahama Botnet) に組み込まれたゾンビPCが、ネット閲覧時に実際に入力したサイト (グーグル、ピーピング、ヤフーなど) とは別のサイトに誘導されました。クリックによる金儲け目的の行為でした。

10月17日 ドイツの学生向けのSNS、シューラー・ファウツェット (schulerVZ) の数十万件もの個人情報が、ネッツポリティーク・オルグ (netzpolitik.org) に流出しました。個人情報は、データ収集プログラム (クローラー) で盗み出された模様です。

10月19日 スウェーデンの裁判所はパイレート・ベイに関わる4名と著作権団体の審理を2010年夏にやり直しにすると声明しました。裁判に関与していた裁判官2人に対して、当裁判への適正が疑われたためです。

10月23日 クリック・フォレンジックス (Click Forensics) 社のレポートによると、2009年第3四半期のクリック詐欺のうち、42.6%はボットネットのコンピュータからの攻撃であることが判明しました。

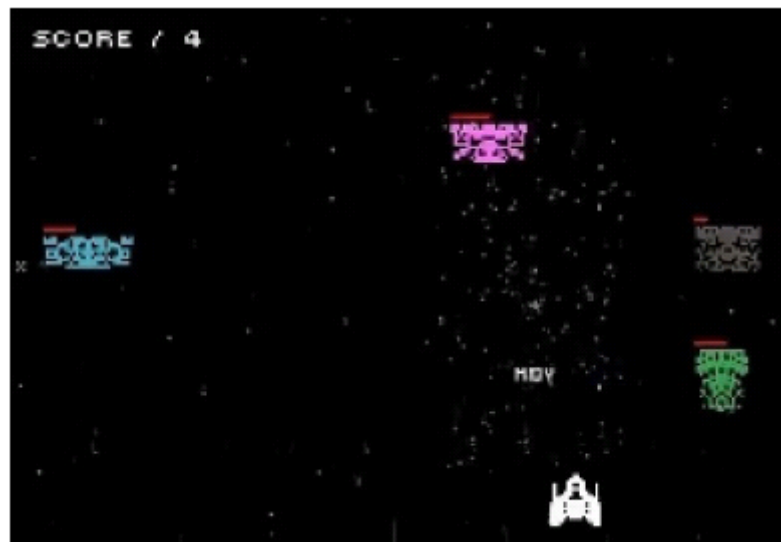
10月31日 ドイツの学生向け SNS シューラー・ファウツェットで大量のユーザーデータを盗み出した罪で2週間前に逮捕されたばかりの20歳の男が獄中で自殺しました。

## 2009年11月

11月1日 ワームの一種であるコンフィッカー (Conficker) による感染が700万を越えました。コンフィッカーはその拡散、潜伏、保護メカニズムにおいて、2009年に最も流行したマルウェアです。

11月3日 イギリスのマンチェスターで20歳のカップルが逮捕されました。二人はスパイウェアのズィーボット (Zbot) を拡散し、オンラインショッピング情報、クレジットカード情報、各種パスワードなどを収集しました。ヨーロッパにおいてはこの種の逮捕は初でした。

11月5日 スペースインベーダーに似せて開発されたマック用ゲーム「ルーズ/ルーズ」では、インベーダーを撃退するたびに、文書フォルダからファイルが削除されました。ただし開発者は、ゲーム開始前に警告メッセージを表示させました。



11月10日 クープフェイスの作者が、フェイスブックなどのSNSで人間のようにふるまう亜種をプログラミングしました。この亜種はアカウント登録、プロフィール作成、友達リクエストの送信、他のユーザーのページへの書き込みを行いました。

11月17日 イギリスのティーモバイル (T-Mobile) 社員によるデータ販売スキャンダルが発覚しました。複数の社員が何千もの顧客データをデータ取引業者に売却した模様です。

11月20日 インターネット・エクスプローラーのバージョン5~7へのゼロデイエクスプロイトが公表されました。コードが有害な環境は、全環境・コンピュータを対象としないも、クラッカー側はコードの最適化に取り組みました。

11月24日 オンライン犯罪撲滅へ。クレジットカード情報、各種アクセスデータ、銀行口座情報、不正ソフトの交換や売買の疑いで、ドイツ・オーストリアの警察官200人が50の住居に一斉ガサ入れ、4人を逮捕しました。ゾンビPCの数が10万台クラスのボットネットも運営していた模様です。

11月24日 アラン・ラルスキー (Alan Ralsky, 64歳、男性、通称スパム界のゴッドファーザー) に対し、懲役4年3ヶ月、執行猶予5年、罰金250万ドルの判決がアメリカで言い渡されました。彼は、複数の共犯者と共に大量スパム送信を関わっていた人物でした。

11月25日 スпам対策の一環として、韓国がSMS送信を制限しました。携帯電話からのSMS送信は、1

日最大 500 回へと制限を設けられました。韓国ではスパム送信者への刑罰は比較的厳しいのですが、スパムの量は膨大でした。統計によると、韓国国民の 98% が携帯電話を所持し、台数は 4770 万台に上ります。

11 月 27 日 ワールド・オブ・ウォークラフト (World of Warcraft) のユーザーを対象とした大規模スパムが発生しました。スパムには画像や動画ファイルが添付され、ユーザーがこれを開くとトロイの木馬に感染、ゲームアカウントを奪われる仕組みでした。

11 月 29 日 英語圏における 2009 年のトップワード 1 位は「ツイッター」でした。2 位は「オバマ」、3 位は「H1N1」、4 位は「スティミュラス」、5 位は「バンパイア」でした。

## 2009年12月

12 月 4 日 バーチャルホテルの「ハッポ」(Habbo) のユーザーが大規模なフィッシング攻撃の被害にあいました。攻撃者は、ブログにも詐欺に導くエントリーを大量に残し、ユーザーのアクセスデータやクレジットカード情報を盗み出しました。



12 月 6 日 ヨーロッパ最大のハッカー協会であるケイオス・コンピュータ・クラブ (Chaos Computer Club) によると、ドイツの学童生徒ポータルサイトのヘフト・デ (haefft.de) はデータ詐欺に対して十分に保護されていないと発表しました。パスワードや高度な知識や技術なしでも、コミュニティの一部として移動し、データを盗み出すことが可能であると発表後、同サイトはネットワークから外されました。

12 月 8 日 無線 LAN のセキュリティを破るサービス。アメリカのある企業が 400 ものクラウド CPU と辞書攻撃を使い、WPA を 20 分以内に破るサービスを提供しました。価格は 34 ドル。

12 月 15 日 アドビ・リーダーとアクロバット 9.2 よりも古いバージョンの「ドック・メディア・ニュープレイヤー」(Doc.media.newPlayer) 機能において、未知の脆弱性が発見されました。この脆弱性が悪用されると、システムを乗っ取られる危険性があり、アドビは 2010 年 1 月 12 日にパッチを発表すると告知しました。

12 月 16 日 9 ヶ月もの捜査の結果、映画「Xメン・オリジン・ウルヴァリン (X-Men Origins: Wolverine)」の不正コピー者がニューヨークで逮捕されました。同容疑者はファイル共有サービスを利用し、映画公開前に映画ファイルを拡散。実際にファイルを盗み出した容疑者は別に存在する模様も、詳細は今のところ不明です。

12 月 17 日 ツイッターへの攻撃。不正な DNS エントリーを悪用することによってホームページを停止させ、「イラン・サイバー・アーミー」(Iranian Cyber Army) のサイトを表示させました。ツイッター側の説明によると、ツイッター・ユーザーにも攻撃が行われた可能性がある模様。その他の被害については不明です。